

日本国特許庁  
JAPAN PATENT OFFICE

#4  
Jc973 U.S. PTO  
09/988156  
11/19/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日  
Date of Application:

2000年11月17日

出願番号  
Application Number:

特願2000-351510

出願人  
Applicant(s):

株式会社日立製作所

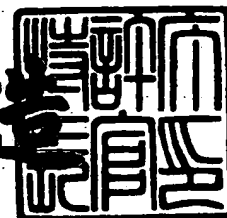
T. Owada et al  
fld 11-19-01  
TSM-17  
M03-684-1120

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年11月 9日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3098683

【書類名】 特許願  
【整理番号】 HK13584000  
【提出日】 平成12年11月17日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G06F 5/00

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 大和田 徹

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 北原 潤

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 朝日 猛

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100087170

【弁理士】

【氏名又は名称】 富田 和子

【電話番号】 045(316)3711

【手数料の表示】

【予納台帳番号】 012014

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】明細書

【発明の名称】情報処理装置、表示装置、デジタルコンテンツ配布システム、および、デジタルコンテンツ配布・出力方法

【特許請求の範囲】

【請求項 1】

処理装置および出力装置を少なくとも備えた情報処理装置において、

上記処理装置は、

デジタルコンテンツに対して、上記出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、

暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備え

上記出力装置は、

上記処理装置から転送されるデジタルコンテンツを入力する入力手段と、

入力したデジタルコンテンツに対して、上記処理装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、

暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備えたことを特徴とする情報処理装置。

【請求項 2】

処理装置および出力装置を少なくとも備えた情報処理装置において、

上記処理装置は、

デジタルコンテンツの一部分に対して、上記出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、

一部分が暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備え、

上記出力装置は、

上記処理装置から転送されるデジタルコンテンツを入力する入力手段と、

入力したデジタルコンテンツに対して、上記処理装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、

暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備えたこと

を特徴とする情報処理装置。

【請求項 3】

処理装置および出力装置を少なくとも備えた情報処理装置において、

上記処理装置は、

暗号化されたデジタルコンテンツを入力する入力手段と、

入力したデジタルコンテンツに対して、該デジタルコンテンツを復号するための暗号鍵情報を用いて復号処理を施す復号処理手段と、

復号後のデジタルコンテンツの一部分に対して、上記出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、

暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備え

上記出力装置は、

上記処理装置から転送されるデジタルコンテンツを入力する入力手段と、

入力したデジタルコンテンツに対して、上記処理装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、

暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備えたことを特徴とする情報処理装置。

【請求項 4】

暗号化されたデジタルコンテンツを入力する入力手段と、

入力したデジタルコンテンツに対して、該デジタルコンテンツを復号するための暗号鍵情報を用いて復号処理を施す復号処理手段と、

復号後のデジタルコンテンツの一部分に対して、該デジタルコンテンツの出力先の出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、

一部分が暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備えたことを特徴とする情報処理装置。

【請求項 5】

請求項 3 または 4 記載の情報処理装置であって、

上記入力手段が入力するデジタルコンテンツは、

平文時のデジタルコンテンツのフォーマット単位を 1 単位とし、これら

の単位の一部の単位が暗号化対象となるようにして暗号化されていることを特徴とする情報処理装置。

【請求項 6】

請求項 2, 3, 4 または 5 記載の情報処理装置であって、

上記暗号処理手段は、

平文時のデジタルコンテンツのフォーマッティング単位を 1 単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。

【請求項 7】

請求項 2, 3, 4 または 5 記載の情報処理装置であって、

上記出力装置が音声再生装置である場合に、

上記暗号処理手段は、

上記音声再生装置に出力する音声データについて、複数サンプル分の音声データを 1 単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。

【請求項 8】

請求項 2, 3, 4 または 5 記載の情報処理装置であって、

上記出力装置が表示装置である場合に、

上記暗号処理手段は、

上記表示装置に出力する表示データのライン方向に、複数ライン分の表示データを 1 単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すか、または、上記表示装置に出力する表示データのカラム方向に、複数カラム分の表示データを 1 単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。

【請求項 9】

請求項 2, 3, 4 または 5 記載の情報処理装置であって、

上記出力装置が表示装置である場合に、

上記暗号処理手段は、

上記表示装置に出力する表示データの 1 画素分のデータを 1 単位とし、これら

の単位の一部または全部について、各々、その一部分を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。

【請求項 1 0】

暗号化された表示データを入力する入力手段と、

入力した表示データに対して、該表示データの転送元の情報処理装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、

暗号化部分を復号後の表示データを表示する表示手段とを備えたことを特徴とする表示装置。

【請求項 1 1】

請求項 1 0 記載の表示装置であって、

上記入力手段が入力するデジタルコンテンツは、

平文時の表示データのライン方向に、複数ライン分の表示データを 1 単位とし、これらの単位の一部の単位が暗号処理の処理対象となるようにして暗号化されているか、または、平文時の表示データのカラム方向に、複数カラム分の表示データを 1 単位とし、これらの単位の一部の単位が暗号処理の処理対象となるようにして暗号化されていることを特徴とする表示装置。

【請求項 1 2】

請求項 1 0 記載の情報処理装置であって、

上記入力手段が入力するデジタルコンテンツは、

平文時の表示データの 1 画素分のデータを 1 単位とし、これらの単位の一部または全部について、各々、その一部分が暗号処理の処理対象となるようにして暗号化されていることを特徴とする表示装置。

【請求項 1 3】

デジタルコンテンツを配布するデジタルコンテンツ配布装置と、デジタルコンテンツ配布装置から配布されるデジタルコンテンツを出力装置に転送して出力する情報処理装置とを備えたデジタルコンテンツ配布システムにおいて、

上記デジタルコンテンツ配布装置は、

上記情報処理装置と共有する第 1 の暗号鍵情報を用いて一部分が暗号化されたデジタルコンテンツを蓄積している蓄積手段と、

蓄積しているデジタルコンテンツを上記情報処理装置に配布する配布手段とを備え、

上記情報処理装置は、

上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツを入力する入力手段と、

入力したデジタルコンテンツ中の暗号化部分に対して、上記第 1 の暗号鍵情報を用いて復号処理を施す復号処理手段と、

暗号化部分を復号後のデジタルコンテンツの一部に対して、上記出力装置と共有する第 2 の暗号鍵情報を用いて暗号処理を施す暗号処理手段と、

暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備え、

上記出力装置は、

上記情報処理装置から転送されるデジタルコンテンツを入力する入力手段と、

入力したデジタルコンテンツ中の暗号化部分に対して、上記第 2 の暗号鍵情報を用いて復号処理を施す復号処理手段と、

暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備え、

上記デジタルコンテンツ配布装置の暗号処理手段、および、上記情報処理装置の暗号処理手段は、

平文時のデジタルコンテンツのフォーマット単位を 1 単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とするデジタルコンテンツ配布システム。

【請求項 1 4】

デジタルコンテンツを配布するデジタルコンテンツ配布装置と、デジタルコンテンツ配布装置から配布されるデジタルコンテンツを出力装置に転送して出力する情報処理装置とを備えたデジタルコンテンツ配布システムにおいて、上記デジタルコンテンツ配布装置から上記情報処理装置へデジタルコンテンツを配布して上記出力装置で出力する方法であって、

上記デジタルコンテンツ配布装置が、上記情報処理装置と共有する第 1 の暗号鍵情報を用いて一部分が暗号化されたデジタルコンテンツを、上記情報処理装置



に配布し、

上記情報処理装置が、上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツ中の暗号化部分に対して、上記第 1 の暗号鍵情報を用いて復号処理を施し、暗号化部分を復号後のデジタルコンテンツの一部に対して、上記出力装置と共有する第 2 の暗号鍵情報を用いて暗号処理を施してから、暗号化後のデジタルコンテンツを上記出力装置に転送し、

上記出力装置が、上記情報処理装置から転送されるデジタルコンテンツ中の暗号化部分に対して、上記第 2 の暗号鍵情報を用いて復号処理を施し、暗号化部分を復号後のデジタルコンテンツのを出力し、

上記デジタルコンテンツ配布装置が配布するデジタルコンテンツ、および、上記情報処理装置が転送するデジタルコンテンツは、

平文時のデジタルコンテンツのフォーマッティング単位を 1 単位とし、これらの単位中の一部の単位が暗号化対象となるようにして暗号化されていることを特徴とするデジタルコンテンツ配布・出力方法。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、著作権保護が必要なデジタルコンテンツを扱う技術に関し、特に、複製による不正使用を防ぎ、かつ、正当な使用権利を持たないユーザの視聴覚欲求を刺激する形での利用を可能としながら、デジタルコンテンツを配布し、配布先の情報処理装置で出力する方法に関する。

##### 【0002】

#### 【従来の技術】

近年、映像や音声などの高付加価値な情報をデジタル形式で配布する要求が高まっており、デジタルコンテンツの著作権保護を図るために、不正コピーの防止が重要視されてきている。すなわち、デジタルコンテンツは、容易にコピーできる上、コピーしても品質が劣化しないので、既に不正コピーによる著作権の侵害等の弊害が生じてきている。

##### 【0003】

コピー防止手段の1つとしては、一般に、デジタルコンテンツの暗号化が用いられており、正当な暗号鍵情報を入手したユーザのみが、暗号化されたデジタルコンテンツを復号し、その中身を確認することができるようにしている。

【0004】

【発明が解決しようとする課題】

しかしながら、デジタルコンテンツを単純に暗号化した場合、暗号化されたデジタルコンテンツは、正当な暗号鍵情報がないと全く視聴することができなくなってしまう。

【0005】

これは、デジタルコンテンツが何らかのフォーマットに従ってフォーマットイングされているにも関わらず、フォーマットを無視した単純な暗号化が行われることにより、デジタルコンテンツのデータ構造が破壊されてしまい、デジタルコンテンツを再生するソフトウェアやハードウェアがデータ構造を全く解釈できなくなるからである。

【0006】

そこで、ユーザは、デジタルコンテンツを購入するなどして、正当な暗号鍵情報を入手しない限り、その中身を確認することができず、ユーザにとってはデジタルコンテンツ購入の敷居が高くなってしまう。

【0007】

このような問題を解決するためには、デジタルコンテンツの権利保護を大前提にしつつも、ユーザの視聴覚欲求を刺激する形でデジタルコンテンツを配布するようにすることが好ましい。

【0008】

また、従来、デジタルコンテンツの暗号化は、ユーザの情報処理装置に到達するまでの経路についてのみ行われており、情報処理装置において、表示装置などの最終出力装置へ出力する際の経路については、暗号化による著作権保護の対象とはなっていない。

【0009】

近年、従来のCRT (Cathode-Ray Tube) 表示装置のようなアナログ入力之最

終出力装置に代わり、液晶表示装置のようなデジタル入力の最終出力装置が一般化しつつあることから、このような最終出力装置へ出力する際の経路で、デジタルコンテンツの不正コピーが行われる恐れがある。

【0010】

そこで、本発明の目的は、情報処理装置において、デジタルコンテンツを最終的に出力する際の経路での不正コピーを防止することを可能にすることにある。

【0011】

また、本発明のもう1つの目的は、情報処理装置において、デジタルコンテンツの権利を保護すると共に、ユーザの視聴覚欲求を刺激することにより、デジタル時コンテンツの配布または販売を促進することを可能にすることにある。

【0012】

【課題を解決するための手段】

上記目的を達成するために、本発明は、処理装置および出力装置を少なくとも備えた情報処理装置において、上記処理装置が、上記出力装置と共有する暗号鍵情報を用いて暗号化したデジタルコンテンツを、上記出力装置に転送し、上記出力装置が、上記処理装置から転送されるデジタルコンテンツに対して、上記暗号鍵情報を用いて復号処理を施すようにしている。

【0013】

そして、特に、本発明では、もう1つの目的を達成するために、上記処理装置から上記出力装置に転送されるデジタルコンテンツが、平文時のデジタルコンテンツのフォーマット単位を1単位とし、これらの単位の一部の単位が暗号化対象となるようにして暗号化されたものであるようにしている。

【0014】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。

【0015】

図1は、本実施形態に係るデジタルコンテンツ配布システムの概略構成図である。

【0016】

図中、100はデジタルコンテンツ配布装置、101は情報処理装置、102は情報処理装置本体、103は表示装置である。

## 【0017】

本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツ配布装置100によってデジタルデータとして配布される高付加価値コンテンツの権利保護を大前提としている。すなわち、本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツ配布装置100と情報処理装置本体102との間を転送されるデジタルコンテンツ（配布データ）、および、情報処理装置本体102と表示装置103との間を転送されるデジタルコンテンツ（表示データ）が、各々、デジタルデータであるようなものを対象にしており、これらを暗号化することで保護を図っている。

## 【0018】

そして、本実施形態に係るデジタルコンテンツ配布システムは、ユーザの視聴覚欲求を刺激する形でデジタルコンテンツを配布可能とすることを目的としている。すなわち、本実施形態に係るデジタルコンテンツ配布システムは、暗号化されたデジタルコンテンツで、ユーザの視聴覚要求を刺激することを可能とするものである。

## 【0019】

具体的には、デジタルコンテンツ配布装置100と情報処理装置本体102との間を転送されるデジタルコンテンツは、例えば、J P E G (Joint Photographic Experts Group) やM P E G (Moving Picture Experts Group) などの、予め決められた圧縮方式でフォーマットされたデジタルデータが、例えば、D E S (Data Encryption Standard) などの、予め決められた暗号方式で暗号化された暗号化データである。

## 【0020】

ここで、デジタルコンテンツ配布装置100は、ネットワークを経由してデジタルコンテンツを配布するネットワーク装置であっても、例えば、光ディスク媒体や磁気ディスク媒体などの、デジタルコンテンツが記録された記録媒体であってもよい。

## 【 0 0 2 1 】

すなわち、デジタルコンテンツ配布装置 1 0 0 によって配布されるデジタルコンテンツは、デジタルコンテンツ配布装置 1 0 0 から配布される時点で暗号化されていればよく、暗号処理を施すのがデジタルコンテンツ配布装置 1 0 0 でなくてもよい。

## 【 0 0 2 2 】

さて、図 1 に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、デジタルコンテンツ配布装置 1 0 0 および情報処理装置本体 1 0 2 は、何らかの方法によって、デジタルコンテンツ（配布データ）を暗号化／復号化するための暗号鍵情報 1 0 4 を共有する機能を有している。

## 【 0 0 2 3 】

暗号鍵情報 1 0 4 を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよい。

## 【 0 0 2 4 】

例えば、デジタルコンテンツの暗号化に用いられた暗号鍵情報 1 0 4 を管理しているネットワーク装置から、情報処理装置本体 1 0 2 が暗号鍵情報 1 0 4 を入手するという方法が挙げられる。このとき、ネットワーク装置が、情報処理装置本体 1 0 2 の公開鍵情報を用いて暗号鍵情報 1 0 4 を暗号化し、情報処理装置本体 1 0 2 が、自身の秘密鍵情報で復号するようにする。

## 【 0 0 2 5 】

また、例えば、磁気ディスク媒体に記録されているデジタルコンテンツ（暗号化済み）の暗号化に用いられた暗号鍵情報 1 0 4 を、情報処理装置本体 1 0 2 の製造時に、情報処理装置本体 1 0 2 の内部の不揮発性記憶装置に記録しておくという方法が挙げられる。

## 【 0 0 2 6 】

同様に、図 1 に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、情報処理装置本体 1 0 2 および表示装置 1 0 3 は、何らかの方法によって、デジタルコンテンツ（表示データ）を暗号化／復号化するための暗号鍵情報 1 0 5 を共有する機能を有している。

【0027】

暗号鍵情報105を共有する方法についても、暗号鍵情報104を共有する方法と同様に、様々な方法が公知技術となっており、どのような方法を採用してもよい。

【0028】

例えば、情報処理装置本体102がデジタルコンテンツの暗号化に用いた暗号鍵情報105を、表示装置103が情報処理装置本体102から入手するという方法が挙げられる。このとき、情報処理装置本体102が、表示装置103の公開鍵情報を用いて暗号鍵情報105を暗号化し、表示装置103が、自身の秘密鍵情報で復号するようにする。

【0029】

また、例えば、暗号鍵情報105を、情報処理装置本体102および表示装置103の製造時に、各々の内部の不揮発性記憶装置に記録しておくという方法が挙げられる。

【0030】

また、図1に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、情報処理装置本体102は、

(1) デジタルコンテンツ配布装置100から配布されるデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報104を用いて復号処理106を施す復号機能、

(2) 暗号化部分を復号後のデジタルコンテンツの展開処理107を行う展開機能、

(3) 展開したデジタルコンテンツを、表示装置103が要求するビットレートで出力するための表示データに変換する表示制御処理108を行う表示制御機能、

(4) 表示データの一部に対して、暗号鍵情報105を用いて暗号処理109を施す暗号機能、  
を有している。

【0031】

また、図 1 に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、表示装置 1 0 3 は、

(1) 情報処理装置本体 1 0 2 の暗号機能によって暗号化された表示データ中の暗号化部分に対して、暗号鍵情報 1 0 5 を用いて復号処理 1 1 0 を施す復号機能

(2) 暗号化部分を復号後の表示データの表示処理 1 1 1 を行う表示機能、  
を有している。

#### 【 0 0 3 2 】

次に、本実施形態に係るデジタルコンテンツ配布システムの概略動作について、図 2 を用いて説明する。

#### 【 0 0 3 3 】

図 2 は、本実施形態に係るデジタルコンテンツ配布システムの概略動作フローチャートである。

#### 【 0 0 3 4 】

図 2 において、まず、デジタルコンテンツ配布装置 1 0 0 および情報処理装置本体 1 0 2 は、何らかの方法によって、デジタルコンテンツ（配布データ）を暗号化／復号化するための暗号鍵情報 1 0 4 を共有する（ステップ 2 0 1）。上述したように、暗号鍵情報 1 0 4 を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよいので、ここでは規定しない。

#### 【 0 0 3 5 】

続いて、デジタルコンテンツ配布装置 1 0 0 は、情報処理装置本体 1 0 2 へ、暗号鍵情報 1 0 4 を用いて一部分が暗号化されたデジタルコンテンツを配布する（ステップ 2 0 2）。上述したように、デジタルコンテンツ配布装置 1 0 0 によって配布されるデジタルコンテンツは、デジタルコンテンツ配布装置 1 0 0 から配布される時点で暗号化されていればよく、暗号処理を施すのがデジタルコンテンツ配布装置 1 0 0 でなくてもよい。

#### 【 0 0 3 6 】

続いて、情報処理装置本体 1 0 2 は、デジタルコンテンツ配布装置 1 0 0 から配布されたデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報 1 0 4 を用

いて復号処理 1 0 6 を施す（ステップ 2 0 3）。ステップ 2 0 3 の処理によって、情報処理装置本体 1 0 2 は、その内部に、平文のデジタルコンテンツを得ることとなる。

#### 【 0 0 3 7 】

続いて、情報処理装置本体 1 0 2 は、ステップ 2 0 3 の処理で得られたデジタルコンテンツの展開処理 1 0 7 を行う（ステップ 2 0 4）。例えば、ステップ 2 0 3 の処理で得られたデジタルコンテンツが M P E G 方式でフォーマットされている M P E G データである場合には、ステップ 2 0 4 の処理によって、情報処理装置本体 1 0 2 は、その内部に、毎秒 3 0 フレームからなる動画データを得ることとなる。

#### 【 0 0 3 8 】

続いて、ステップ 2 0 4 の処理で得られた動画データを含む表示データに対して、表示装置 1 0 3 が要求するビットレートで出力するための表示制御処理 1 0 8 を行う（ステップ 2 0 5）。例えば、表示装置 1 0 3 が T F T (Thin Film Transistor) 液晶表示装置の場合は、ステップ 2 0 5 の処理では、情報処理装置本体 1 0 2 は、毎秒 6 0 ～ 7 0 フレーム程度のシーケンシャルな表示データを生成する。

#### 【 0 0 3 9 】

続いて、情報処理装置本体 1 0 2 および表示装置 1 0 3 は、何らかの方法によって、デジタルコンテンツ（表示データ）を暗号化／復号化するための暗号鍵情報 1 0 5 を共有する（ステップ 2 0 6）。上述したように、暗号鍵情報 1 0 5 を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよいので、ここでは規定しない。

#### 【 0 0 4 0 】

続いて、情報処理装置本体 1 0 2 は、ステップ 2 0 5 の処理で生成した表示データ中の一部分に対して、暗号鍵情報 1 0 5 を用いて暗号処理 1 0 9 を施す（ステップ 2 0 7）。ステップ 2 0 7 の処理によって、情報処理装置本体 1 0 2 は、その内部に、一部分が暗号化された表示データを得ることとなる。

#### 【 0 0 4 1 】



続いて、情報処理装置本体102は、表示装置103へ、一部分が暗号化された表示データを出力する（ステップ208）。

【0042】

続いて、表示装置103は、情報処理装置本体102から出力された表示データ中の暗号化部分に対して、暗号鍵情報105を用いて復号処理110を施す（ステップ209）。ステップ209の処理によって、表示装置103は、その内部に、平文の表示データを得ることとなる。

【0043】

続いて、表示装置103は、ステップ209の処理によって得られた表示データの表示処理111を行う（ステップ210）。ステップ210の処理によって、ステップ204の処理によって得られた動画像データを含む表示データが表示されることとなる。

【0044】

以上、ステップ201～ステップ210の処理によって、デジタルコンテンツ配布装置100から配布されるデジタルコンテンツが、表示装置103で表示されることとなる。

【0045】

なお、以下では、本実施形態に係るデジタルコンテンツ配布システムの動作のうち、ステップ201～ステップ204の処理によって実現される動作を、「配布経路暗号化」動作と称し、ステップ205～ステップ210の処理によって実現される動作を、「出力経路暗号化」動作と称する。

【0046】

また、ステップ206の処理は、配布経路暗号化動作に先立って行われても、並行して行われてもよい。また、ステップ205，ステップ206，ステップ207の処理は、情報処理装置101の構成によっては順番が逆転してもよい。

【0047】

次に、配布経路暗号化動作の詳細について説明する。

【0048】

まず、本実施形態に係る情報処理装置101の概略動作について、図3を用い

て説明する。

【0049】

図3は、本実施形態に係る情報処理装置101の概略構成図である。

【0050】

図3では、パーソナルコンピュータ（PC）などの情報処理装置101のうち、表示に関する部分であって、かつ、配布経路暗号化動作に関する部分のみを示している。

【0051】

図中、102は情報処理装置本体、103は表示装置、104は暗号鍵情報、301は中央演算装置（CPU：Central Processing Unit）、302はシステムメモリ、303は表示制御装置、304は表示メモリ、305は入力制御装置、306は通信制御装置、307はバス、308は復号処理部、309はコンテンツ展開処理部である。

【0052】

図3において、デジタルコンテンツ配布装置100がネットワーク装置である場合には、通信制御装置306が、CPU301の指示に従って、デジタルコンテンツを入力する。また、デジタルコンテンツ配布装置100が記録媒体である場合には、入力制御装置305が、CPU301の指示に従って、デジタルコンテンツを入力する。通信制御装置306または入力制御装置305が入力したデジタルコンテンツは、CPU301の指示に従って、バス307を介して表示制御装置303に入力される。

【0053】

表示制御装置303においては、復号処理部308が、入力したデジタルコンテンツ中の暗号化部分に対して、表示制御装置303の内部に保持されている暗号鍵情報104を用いて復号処理106を施し、表示制御装置303の内部に、平文のデジタルコンテンツを得る。続いて、コンテンツ展開処理部309が、復号処理部308が復号したデジタルコンテンツの展開処理107を行い、表示制御装置303の内部に、展開されたデジタルコンテンツを得る。

【0054】

ここまでの動作が配布経路暗号化動作に相当している。その後の出力経路暗号化動作の詳細については後述する。

## 【 0 0 5 5 】

なお、復号処理部 3 0 8 およびコンテンツ展開処理部 3 0 9 は、表示制御装置 3 0 3 内にハードウェアとして実装されるようにしてもよいし、また、表示制御装置 3 0 3 内に独自の CPU およびメモリを設け、ソフトウェアとして実装されるようにしてもよい。

## 【 0 0 5 6 】

次に、配布経路暗号化動作で、デジタルコンテンツ配布装置 1 0 0 から配布されるデジタルコンテンツの暗号化方法の一例について、図 5 および図 6 を用いて説明する。

## 【 0 0 5 7 】

図 5 は、デジタルコンテンツ配布装置 1 0 0 から配布されるデジタルコンテンツの暗号化方法の一例を示す説明図であり、図 6 は、図 5 に示す暗号化方法で暗号化されたデジタルコンテンツを表示装置 1 0 3 で表示した場合の表示イメージを示す説明図である。

## 【 0 0 5 8 】

図 5 および図 6 では、デジタルコンテンツが M P E G データである場合を例にしている。

## 【 0 0 5 9 】

M P E G 方式による圧縮では、例えば、1 フレーム  $m \times n$  画素、毎秒  $k$  フレームから構成される動画データは、I ピクチャ形式、P ピクチャ形式、B ピクチャ形式の 3 つの形式に分類される。

## 【 0 0 6 0 】

## (1) I ピクチャ形式

I ピクチャ形式では、1 フレーム  $m \times n$  画素の画像データは、 $8 \times 8$  画素の複数のブロックに分割され、各ブロックごとに直交変換処理が施されて周波数領域データに変換された後、量子化されてデータ圧縮が行われる。I ピクチャデータでは、元フレーム内のデータのみを対象にした符号化がなされており、I ピクチャ

ャデータからは、展開処理によって1枚のフレームデータが得られる。

【0061】

(2) Pピクチャ形式

Pピクチャ形式では、順方向のフレーム間予測を行ったデータ圧縮が行われる。Pピクチャデータでは、Iピクチャとの差分情報を用いた符号化がなされており、元フレームの復元には、Pピクチャデータ、元画となるIピクチャデータが必要となる。すなわち、Pピクチャデータのみでは画像データは得られない。

【0062】

(3) Bピクチャ形式

Bピクチャ形式では、双方向のフレーム間予測を行ったデータ圧縮が行われる。Bピクチャデータでは、IピクチャとPピクチャとの間の差分情報を用いた符号化がなされており、元フレームの復元には、Pピクチャデータ、元画となるIピクチャデータ、Bピクチャデータが必要となる。すなわち、Bピクチャデータのみでは画像データは得られない。

【0063】

また、1ピクチャデータの符号割り当て量は、図5に示すように、Iピクチャ、Pピクチャ、Bピクチャの順に小さくなる。動画像データは、フレームごとに、例えば、IBB, PBB, PBB, IBB, PBB, PBBなどの順番に符号化される。

【0064】

このような性質を持ったMPEGデータの暗号化方法としては、以下の3つの方法が考えられる。

【0065】

(1) 第1の暗号化方法

第1の暗号化方法としては、Iピクチャデータのみを暗号化するという方法がある。第1の暗号化方法は、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となるブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

## 【0066】

まず、前者の方法（圧縮単位となるブロックごとに暗号化を施す／施さないという方法）について説明すると、例えば、図6（a）に示す元画像に対して、本方法による暗号化を行う際には、ブロックを暗号処理の処理対象とし、あるブロックには暗号処理を施し、あるブロックには暗号処理を施さないようにする。

## 【0067】

本方法により暗号化されたMPEGデータは、暗号鍵情報104を用いた復号処理を施さなければ、表示装置103に表示される際のイメージは、図6（b）に示すようになる。本方法では、暗号化を施すブロック数を増減させることで、元画像の汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

## 【0068】

次に、後者の方法（高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法）について説明すると、例えば、図6（a）に示す元画像に対して、本方法による暗号化を行う際には、ブロック内の低周波領域データを暗号処理の処理対象とし、各ブロック中の低周波領域データには暗号処理を施し、高周波領域データには暗号処理を施さないようにする。本方法により暗号化されたMPEGデータは、暗号鍵情報104を用いた復号処理を施さなければ、表示装置103に表示される際のイメージは、図6（c）に示すようになる。

## 【0069】

低周波数領域データを暗号化すると、図6（c）に示すように、元画像は大きく汚染され、元画像を観測するのは困難となるが、高周波数領域データを暗号化すると、図示していないが、元画像にノイズが重畳されたイメージとなる。

## 【0070】

本方法では、暗号化を施す周波数領域を選択することで、元画像の汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。また、全てのブロックを暗号処理の処理対象としなくても、一部のブロックを暗号処理の処理対象としてもよい。

## 【0071】

第1の暗号化方法によってIピクチャデータのみを暗号化した場合、暗号鍵情報104がないとIピクチャデータを復元することができず、従って、図5に示すように、Iピクチャデータの差分情報であるPピクチャデータおよびBピクチャデータも、暗号化されてはいないが、これらを展開することも不可能となる。例えば、IBB, PBB, PBB, IBB, PBB, PBBの順番に符号化された動画データは、暗号鍵情報104がない場合には、×××, ×××, ×××, ×××, ×××, ×××(×は正常な復号・展開の失敗を意味する。)となって、全てのフレーム共に正常な元画像が得られない。

## 【0072】

## (2) 第2の暗号化方法

第2の暗号化方法としては、Pピクチャデータのみを暗号化するという方法がある。第2の暗号化方法も、第1の暗号化方法と同様に、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となるブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

## 【0073】

第2の暗号化方法によってPピクチャデータのみを暗号化した場合、暗号鍵情報104がないとPピクチャデータを復元することができず、従って、図5に示すように、Iピクチャデータ、Pピクチャデータの差分情報であるBピクチャデータも、暗号化されてはいないが、これを展開することも不可能となる。例えば、IBB, PBB, PBB, IBB, PBB, PBBの順番に符号化された動画データは、暗号鍵情報104がない場合には、I××, ×××, ×××, I××, ×××, ×××(×は正常な復号・展開の失敗を意味する。)となって、得られる正常な画像フレームはIピクチャデータのみとなる。

## 【0074】

## (3) 第3の暗号化方法

第3の暗号化方法としては、Bピクチャデータのみを暗号化するという方法がある。第3の暗号化方法も、第1の暗号化方法と同様に、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となる

ブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

#### 【 0 0 7 5 】

第3の暗号化方法によってBピクチャデータのみを暗号化した場合、図5に示すように、暗号鍵情報104がないとBピクチャデータを復元することができない。例えば、I B B, P B B, P B B, I B B, P B B, P B Bの順番に符号化された動画像データは、暗号鍵情報104がない場合には、I × ×, P × ×, P × ×, I × ×, P × ×, P × × (Xは正常な復号・展開の失敗を意味する。) となって、得られる正常な画像フレームはIピクチャデータおよびPピクチャのみとなる。

#### 【 0 0 7 6 】

以上、MPEGデータの暗号化方法として3つの方法を説明したが、これらの方法を任意に組み合わせるようにしてもよい。

#### 【 0 0 7 7 】

本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、デジタルコンテンツを単純に暗号化するのではなく、暗号処理の処理対象とするデータを選択し、一部分のみを暗号化するようにしているので、正当な暗号鍵情報104を有していない場合には、元画像の一部分が汚損した状態となる。一部分が汚損されたデジタルコンテンツは、その価値が損なわれるので、デジタルコンテンツの不正コピーを防止することが可能となり、また、デジタルコンテンツの一部分が開示されるので、ユーザの視聴要求を刺激し、デジタルコンテンツの完全な視聴を促すことが可能となる。

#### 【 0 0 7 8 】

特に、本実施形態に係るデジタルコンテンツ配布システムにおいては、暗号処理の処理対象とするデータを選択する際に、そのフォーマットに着目するようにしている。すなわち、デジタルコンテンツを単なるビット列として暗号処理の処理対象とした場合、ヘッダ、ペイロード、フッタと言ったデータ構造が全て失われてしまい、デジタルコンテンツとして利用することがまったく不可能となってしまうが、本実施形態に係るデジタルコンテンツ配布システムにおいては、デジ

タルコンテンツを単なるビット列として扱うのではなく、暗号処理の処理対象とするデータを、フォーマットの有意味部分に合わせて選択するようにしているので、データ全体ではなく、一部分だけの汚損が可能となっている。

## 【0079】

また、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、データ汚損に、暗号鍵情報104を用いた暗号処理を利用していることから、ユーザの視聴欲求を刺激するために、完全なデジタルコンテンツとは別に汚損デジタルコンテンツを用意する必要がなく、デジタルコンテンツの配布・蓄積に掛かるコストを低減することが可能となる。

## 【0080】

さらに、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、デジタルコンテンツの一部分だけを暗号処理の処理対象とし、デジタルコンテンツ全体に対する暗号処理を避けることによって、暗号処理／復号処理の処理量の軽減も可能となっている。なお、汚損度と処理量とはトレードオフの関係にあり、要求に応じて優先度の変更が容易に可能である。

## 【0081】

以上説明したように、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作によって、デジタルコンテンツの配布経路上で著作権を保護しつつ、ユーザの視聴欲求を刺激することが可能となる。

## 【0082】

なお、本実施形態に係る情報処理装置101は、図3に示す構成ではなく、図7に示す構成にし、図3に示した復号処理部308およびコンテンツ展開処理部309を、ソフトウェアで実現するようにしてもよい。

## 【0083】

図7は、本実施形態に係る情報処理装置101の他の概略構成図である。

## 【0084】

図7でも、図3と同様に、PCなどの情報処理装置101のうち、表示に関する部分であって、かつ、配布経路暗号化動作に関する部分のみを示している。

## 【0085】



図中、図3と同じ構成要素には同じ符号を付与してある。701は不揮発性記憶装置である。

## 【0086】

図7に示す構成の情報処理装置101においては、図3に示した復号処理部308およびコンテンツ展開処理部309の動作を、CPU301がシステムメモリ302上にプログラムをロードして実行することで実現するものである。

## 【0087】

図7において、デジタルコンテンツ配布装置100がネットワーク装置である場合には、通信制御装置306が、CPU301の指示に従って、デジタルコンテンツを入力する。また、デジタルコンテンツ配布装置100が記録媒体である場合には、入力制御装置305が、CPU301の指示に従って、デジタルコンテンツを入力する。通信制御装置306または入力制御装置305が入力したデジタルコンテンツは、CPU301の指示に従って、バス307を介してシステムメモリ302に入力される。

## 【0088】

CPU301は、入力したデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報104を用いて復号処理106を施し、システムメモリ302上に、平文のデジタルコンテンツを得る。続いて、CPU301は、復号したデジタルコンテンツの展開処理107を行い、展開されたデジタルコンテンツを得る。得られたデジタルコンテンツは表示制御装置303に入力される。

## 【0089】

ここで、暗号鍵情報104は、図3を用いた説明では、表示制御装置303の内部に保持されているものとしたが、図7に示す構成の情報処理装置101においては、暗号鍵情報104の共有も、CPU301がシステムメモリ302上にプログラムをロードして実行することで実現するものとする。

## 【0090】

また、本実施形態に係る情報処理装置101は、図3および図7のいずれにおいても、情報処理装置102本体と表示装置103とを備えた構成としているが、情報処理装置本体102と表示装置103が一体化した構成であってもよい。

すなわち、本実施形態に係る情報処理装置 1 0 1 を、いわゆる P D A (Personal Digital Assistant) などと呼ばれる携帯情報端末としてもよい。

【 0 0 9 1 】

一般に、携帯情報端末は、比較的性能の低い C P U や小容量のメモリなどを用いて構成されることが多いので、比較的重い処理である暗号処理は携帯情報端末にとって大きな負担になるという問題がある。

【 0 0 9 2 】

そこで、このような問題がある携帯情報端末を、本実施形態に係るデジタルコンテンツ配布システムで用いるようにすれば、全体ではなく一部分が暗号化されたデジタルコンテンツを扱うことにより、本発明が目的とする、著作権保護とユーザの視聴覚欲求刺激の両立を実現することができる上、暗号処理量の低減による負荷低下効果を得ることができる。特に、携帯情報端末が暗号処理をソフトウェアで実現する場合には、暗号処理用に高性能な C P U や大容量メモリを搭載する必要がなくなり、低コスト化、低消費電力化といった効果が得られる。また、携帯情報端末が暗号処理専用のハードウェアを備えるようにする場合には、暗号処理専用のハードウェアに必要な処理速度が低下することから、低動作速度による低消費電力化、ハードウェア論理の小規模化による低コスト化といった効果が得られる。

【 0 0 9 3 】

ところで、上述の説明では、M P E G データ（動画像データ）を例にしたが、必ずしも動画像データのみを対象としている訳ではない。

【 0 0 9 4 】

例えば、デジタルコンテンツが J P E G データ（静止画像データ）である場合には、上述した I ピクチャデータの暗号化方法と同様の暗号化方法を用いることが可能である。

【 0 0 9 5 】

また、例えば、デジタルコンテンツが M P E G データ（音声データ）である場合には、音声情報に対して帯域分割を施し、分割された周波数成分ごとに独立した符号化を行っていることから、低周波成分のみに対する暗号化／高周波成分の

みに対する暗号化を行うようにしたり、数サンプルおきに暗号化を行うようにしたりすればよい。このようにしてデータ汚損度を制御すれば、適度に耳障りな再生音を生成することが可能となる。

【0096】

さて、次に、出力経路暗号化動作の詳細について説明する。

【0097】

まず、本実施形態に係る情報処理装置101の概略動作について、図4を用いて説明する。

【0098】

図4は、本実施形態に係る情報処理装置101の概略構成図である。

【0099】

図4では、PCなどの情報処理装置101のうち、表示に関する部分であって、かつ、出力経路暗号化動作に関する部分のみを示している。

【0100】

図中、図3と同じ構成要素には同じ符号を付与してある。401は暗号処理部、402は復号処理部、403はデータドライバである。

【0101】

ここでは、表示装置103は、例えば、液晶表示(LCD:Liquid Crystal Display)装置や、デジタル／アナログ変換機能を具備したCRT(Cathode-Ray Tube)装置のような、デジタル入力の表示装置とする。

【0102】

図4において、上述した配布経路暗号化動作によって表示制御装置303の内部に展開されたデジタルコンテンツを含む表示データ(平文表示データ)は、CPU301の指示に従って、表示メモリ304に蓄積される。

【0103】

表示制御装置303においては、暗号処理部401が、表示メモリ304に蓄積された平文表示データを入力し、入力した平文表示データの一部分に対して、表示制御装置303の内部に保持されている暗号鍵情報105を用いて暗号処理109を施し、表示制御装置303の内部に、暗号化された表示データを得る。

得られた暗号化表示データは、表示制御装置303から表示装置103へ入力される。

#### 【0104】

続いて、表示装置103においては、復号処理部402が、入力した暗号化表示データ中の暗号化部分に対して、表示装置103の内部に保持されている暗号鍵情報105を用いて復号処理110を施し、表示装置103の内部に、平文表示データを得る。続いて、データドライバ403が、復号処理部402が復号した平文表示データを、表示画面上の各々の表示画素に供給することで、平文表示データの表示処理111を行う。

#### 【0105】

以上の動作が出力経路暗号化動作に相当している。

#### 【0106】

なお、暗号処理部402は、表示制御装置303内にハードウェアとして実装されるようにしてもよいし、また、表示制御装置303内に独自のCPUおよびメモリを設け、ソフトウェアとして実装されるようにしてもよい。

#### 【0107】

次に、本実施形態に係る表示制御装置303の概略動作について、図8を用いて説明する。

#### 【0108】

図8は、本実施形態に係る表示制御装置303の概略構成図である。

#### 【0109】

図8では、表示制御装置303のうち、出力経路暗号化動作に関する部分のみを示している。

#### 【0110】

図中、801はメモリ制御部、802はタイミング生成部、803はタイミング信号、804はメモリ制御信号、805はメモリアドレス信号、304は表示メモリ、806はLCD制御部、807はLCD制御信号、808は平文表示データ、809はタイミング制御部、810はLCD表示データ、811はシリアル／パラレル変換回路（S／P回路）、812はS／P済LCD表示データ、8

13は暗号化S/P済LCD表示データ、814はパラレル/シリアル変換回路(P/S回路)、815は暗号化LCD表示データ、816は遅延回路、817は遅延済LCD制御信号である。

【0111】

図8において、メモリ制御部801は、タイミング生成部802から送られてくるタイミング信号803を用いて、メモリ制御信号804およびメモリアドレス信号805を生成し、表示メモリ304から平文表示データ808を順次読み出す。

【0112】

一方、LCD制御部806は、タイミング生成部802から送られてくるタイミング信号803を用いて、LCDの表示タイミングを制御するLCD制御信号807を生成する。

【0113】

タイミング制御部809は、表示メモリ304から読み出された平文表示データ809を、LCD制御信号807による表示タイミングに合わせて、LCD表示データ810として送り出す。

【0114】

すなわち、表示メモリ304から読み出された平文表示データ808は、タイミング制御部809によって、LCD制御信号807に同期したLCD表示データ810となる。

【0115】

例えば、LCD制御信号807が、1データ転送クロック同期で1画素分の表示データを転送し、かつ、1画素が16ビットのデータから構成されているとすると、LCD表示データ810は、16ビットデータバスとなる。ここで、暗号処理に、例えば、DESのようなブロック暗号を用いた場合、暗号処理部401は、暗号鍵情報105を用いて、64ビット単位のブロック暗号処理を施すこととなる。

【0116】

両者の処理単位の違いを吸収するために、本実施形態に係る表示制御装置30

3においては、S/P回路812およびP/S回路814を用いている。S/P回路811は、LCD表示データ810のデータ幅（ここでは、16ビット単位）を、暗号処理単位（ここでは、64ビット単位）幅に変換し、S/P済LCD表示データ812として暗号処理部401に供給するものであり、また、P/S回路814は、暗号処理部401によって暗号処理が施された後の暗号化S/P済LCD表示データ813のデータ幅を、LCD表示データ810のデータ幅に変換し、暗号化LCD表示データ815としてデータドライバ403に供給するものである。

## 【0117】

LCD表示データ810のデータ幅と暗号処理部401の暗号処理単位幅とに応じて、S/P回路811およびP/S回路814の構成は異なる。

## 【0118】

図8に示すように、本実施形態に係る表示制御装置303においては、S/P回路811、暗号処理部401、P/S回路814による処理が設けられているので、これらの処理による遅延と同等の遅延を、遅延回路816によって、LCD制御部806が生成したLCD制御信号807に加え、遅延済LCD制御信号817として出力するようにすることで、P/S回路814から出力される暗号化LCD表示データ816が、遅延済LCD制御信号817に同期してデータドライバ403に供給されるようにしている。

## 【0119】

これにより、表示制御装置303による表示タイミング制御の処理途上で、表示データの一部に対して暗号処理を施すこと、すなわち、LCD表示データ810のリアルタイム暗号処理による暗号化LCD表示データ815の作成が可能となる。

## 【0120】

次に、本実施形態に係る表示装置103の概略動作について、図9を用いて説明する。

## 【0121】

図9は、本実施形態に係る表示装置103の概略構成図である。

## 【0122】

図9では、表示装置103が液晶表示装置である場合を例にしており、表示装置103のうち、出力経路暗号化動作に関する部分（すなわち、データドライバ403に相当する液晶駆動ドレイン側ドライバ）のみを示している。

## 【0123】

図中、901は暗号化表示データの取り込み信号（CL2信号）、902は暗号化表示データ、903はLCD駆動電圧を出力するタイミング信号（CL1信号）、904はLCD駆動用電源、905は液晶駆動出力信号、906はラッチアドレスセクタ、907はラッチ回路-1、908はラッチ回路-2、909は回路駆動電圧から液晶駆動電圧へ昇圧するレベルシフタ、910は液晶駆動用の電圧レベルを発生する液晶駆動回路、911はラッチ回路-3、912は平文表示データである。

## 【0124】

図9において、ラッチアドレスセクタ906は、暗号化表示データ902の入力と同期して表示制御装置303から入力したCL2信号901（図8に示した遅延済LCD制御信号817に相当している。）の立下りをカウントすることで、ラッチ回路-1（907）に対するラッチ信号を生成する。

## 【0125】

表示制御装置303から入力した暗号化表示データ902は、ラッチアドレスセクタ906が生成するラッチ信号によって、ラッチ回路-1（907）上に入力順に保持されていく。

## 【0126】

CL1信号903は、表示1ラインごとに入力する水平同期信号であり、CL1信号903の入力によって、ラッチ回路-1（907）上にラッチされた1表示ライン分の暗号化表示データ902は、1ライン表示期間ごとに、1ライン分ずつ、ラッチ回路-2（908）上にラッチされる。

## 【0127】

ラッチ回路-2（908）上にラッチされた1ライン分の暗号化表示データ902は、復号処理部402によって、暗号鍵情報105を用いた復号処理100

が施されて平文表示データ 9 1 2 となり、CL 1 信号 9 0 3 によって、1 ライン表示期間ごとに、1 ライン分ずつ、ラッチ回路 - 3 ( 9 1 1 ) 上にラッチされる。

【 0 1 2 8 】

ラッチ回路 - 3 ( 9 1 1 ) 上にラッチされた 1 ライン分の平文表示データ 9 1 2 は、レベルシフタ 9 0 9 および液晶駆動回路 9 1 0 を介して液晶駆動電圧に変換され、1 ライン表示期間、液晶に印加される。

【 0 1 2 9 】

以上の処理により、1 ラインごとに液晶への表示動作が実行される。

【 0 1 3 0 】

ここで、復号処理に、例えば、DES のようなブロック暗号を用いた場合、復号処理部 4 0 2 は、ラッチ回路 - 2 ( 9 0 8 ) から出力されるビット数を、同時に並列処理可能な分だけ、ブロック単位に並列させる。例えば、液晶駆動ドレイン側ドライバが、1 ライン当たり 1 0 2 4 画素構成で 1 画素当たり 1 8 ビット出力であるとする、1 ライン当たり 1 8 4 3 2 ビットとなるので、6 4 ビット単位 ( DES による処理単位 ) のブロックを 2 8 8 個並列させる。そして、復号処理部 4 0 2 は、暗号鍵情報 1 0 5 を用いて、6 4 ビット単位のブロック復号処理を施すこととなる。

【 0 1 3 1 】

これにより、表示装置 1 0 3 の液晶駆動ドレイン側ドライバによる表示制御の処理途上で、表示データの一部に対して復号処理を施すこと、すなわち、暗号化表示データ 9 1 2 のリアルタイム復号処理による平文表示データ 9 1 2 の作成・表示が可能となる。

【 0 1 3 2 】

なお、本実施形態に係る表示装置 1 0 3 は、図 9 に示す構成ではなく、図 1 0 に示す構成にしてもよい。

【 0 1 3 3 】

図 1 0 は、本実施形態に係る表示装置 1 0 3 の他の概略構成図である。

【 0 1 3 4 】



図 1 0 でも、図 9 と同様に、表示装置 1 0 3 が液晶表示装置である場合を例にしており、表示装置 1 0 3 のうち、出力経路暗号化動作に関する部分（すなわち、データドライバ 4 0 3 に相当する液晶駆動ドレイン側ドライバ）のみを示している。

## 【 0 1 3 5 】

図中、図 9 と同じ構成要素には同じ符号を付与してある。1 0 0 1 は S / P 回路、1 0 0 2 は P / S 回路、1 0 0 3 は S / P 済表示データ、1 0 0 4 は平文表示データである。

## 【 0 1 3 6 】

図 1 0 に示す表示装置 1 0 3 は、暗号化表示データ 9 0 2 のデータ幅が、1 画素当たりのデータビット数とデータ転送クロック（CL 2 信号 9 0 1）とに依存し、復号処理部 4 0 2 の復号処理単位のデータ幅と異なっている場合に、S / P 回路 1 0 0 1 によって、暗号化表示データ 9 0 2 のデータ幅を適切な復号処理単位のデータ幅に変換し、S / P 済表示データ 1 0 0 3 としてから、復号処理部 4 0 2 によって、暗号鍵情報 1 0 5 を用いて復号処理を行い、復号処理によって得られた平文表示データ 1 0 0 4 を、P / S 回路 1 0 0 2 によって、平文表示データ 9 1 2 のデータ幅に変換するようにしたものである。

## 【 0 1 3 7 】

復号処理部 4 0 2 は、最低 1 ブロックを処理できればよく、1 画素当たりの暗号化表示データ 9 0 2 のビット数と CL 2 信号 9 0 1 とに応じて、処理ブロックを並列させるようにしてもよい。

## 【 0 1 3 8 】

以上、表示装置 1 0 3 が液晶表示装置である場合を例にとって、出力経路暗号化動作について説明したが、表示装置 1 0 3 が、例えば、デジタル入力でデジタル / アナログ変換部を具備する CRT 装置である場合でも、デジタル処理を行う途上で、同様の復号処理を行うようにすれば、平文表示データの作成・表示が可能となる。

## 【 0 1 3 9 】

次に、出力経路暗号化動作で、表示制御装置 3 0 3 から出力される表示データ

の暗号化方法の一例について、図 1 1 および図 1 2 を用いて説明する。

【0 1 4 0】

図 1 1 は、表示制御装置 3 0 3 から出力される表示データの暗号化方法の一例を示す説明図であり、暗号化された表示データを表示装置 1 0 3 で表示した場合の表示イメージを示す説明図である。

【0 1 4 1】

図 1 1 では、元画像（本来の平文表示データ）の暗号化方法として、ライン方向に暗号処理を施す暗号化方法と、カラム方向に暗号処理を施す暗号化方法とを示している。

【0 1 4 2】

（１）ライン方向に暗号処理を施す暗号化方法

例えば、図 1 1（a）に示す元画像（本来の平文表示データ）に対して、本方法による暗号化を行う際には、ライン方向に、複数ライン分（例えば、数ライン程度）の表示データを 1 単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すようにする。具体的には、数ライン分の表示データごとに、交互に、暗号処理を施す場合と暗号処理を施さない場合とを繰り返すようにする。

【0 1 4 3】

本方法により暗号化された表示データは、暗号鍵情報 1 0 5 を用いた復号処理を施せば、表示装置 1 0 3 に表示される際のイメージは、図 1 1（a）に示す元画像と同じイメージになるが、暗号鍵情報 1 0 5 を用いた復号処理を施さなければ、表示装置 1 0 3 に表示される際のイメージは、図 1 1（b）に示すように、数ラインおきに数ライン分が汚損された表示データとなる。

【0 1 4 4】

本方法では、1 単位とするライン数を予め決定しておき、決定したライン数ごとに、表示制御装置 3 0 3 の暗号処理部 4 0 1 が選択的に暗号化すると共に、表示装置 1 0 3 の復号処理部 4 0 2 が選択的に復号するようにする。これにより、表示データの一部に対する汚損が可能となり、また、表示制御装置 3 0 3 の暗号処理部 4 0 1 および表示装置 1 0 3 の復号処理部 4 0 2 における暗号／復号処理

量の削減が可能となる。

【0 1 4 5】

また、1単位とするライン数を増減させることで、表示データの汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

【0 1 4 6】

(2) カラム方向に暗号処理を施す暗号化方法

例えば、図11(a)に示す元画像(本来の平文表示データ)に対して、本方法による暗号化を行う際には、カラム方向に、複数カラム分(例えば、数カラム程度)の表示データを1単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すようにする。具体的には、数カラム分の表示データごとに、交互に、暗号処理を施す場合と暗号処理を施さない場合とを繰り返すようにする。

【0 1 4 7】

本方法により暗号化された表示データは、暗号鍵情報105を用いた復号処理を施せば、表示装置103に表示される際のイメージは、図11(a)に示す元画像と同じイメージになるが、暗号鍵情報105を用いた復号処理を施さなければ、表示装置103に表示される際のイメージは、図11(c)に示すように、数カラムおきに数カラム分が汚損された表示データとなる。

【0 1 4 8】

本方法では、1単位とするカラム数を予め決定しておき、決定したカラム数ごとに、表示制御装置303の暗号処理部401が選択的に暗号化すると共に、表示装置103の復号処理部402が選択的に復号するようにする。これにより、表示データの一部に対する汚損が可能となり、また、表示制御装置303の暗号処理部401および表示装置103の復号処理部402における暗号/復号処理量の削減が可能となる。

【0 1 4 9】

また、1単位とするカラム数を増減させることで、表示データの汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

【0 1 5 0】

図12は、表示制御装置303から出力される表示データの暗号化方法の一例を示す説明図であり、図12では、元画像（本来の平文表示データ）中の1画素分の表示データについて、その一部分に対して暗号処理を施す暗号化方法を示している。

【0151】

本方法では、1画素内の表示データ中の上位ビットのみに暗号処理を施すようにするか、または、1画素内の表示データ中の下位ビットのみに暗号処理を施すようにする。

【0152】

上位ビットのみを暗号化し、下位ビットは平文のままとした場合は、表示データの変化量が大きくなる。そこで、暗号化表示データを復号せずに表示装置103上で表示すると、データの汚損度が大きく、表示データの観察は困難となる。

【0153】

また、下位ビットのみを暗号化し、上位ビットは平文のままとした場合は、表示データの変化量は少ない。そこで、暗号化表示データを復号せずに表示装置103上で表示すると、データの汚損度が小さく、画面上のちらつきとして観察されるが、表示データのおおまかな観察は可能である。

【0154】

図12では、1画素分の表示データが8ビットで構成され、ある平文表示データが「55h」であるとしたときに、上位ビットのみを暗号化して「55h」が「e5h」になり、下位ビットのみを暗号化して「55h」が「52h」になった例を示した。このように、上位ビットのみを暗号化する方が、平文表示データからの変化量が大きくなるので、より異なった表示として観測されることとなる。

【0155】

本方法では、上位ビットのみを暗号化するか、または、下位ビットのみを暗号化するかを選択することで、表示データの汚損度合を選択することが可能であり、また、表示制御装置303の暗号処理部401および表示装置103の復号処理部402における暗号／復号処理量の削減が可能となる。

## 【0156】

以上、ライン方向／カラム方向に暗号処理を施す暗号化方法、および、1画素内の表示データ中の上位ビット／下位ビットのみに暗号処理を施す暗号化方法について説明したが、これらの方法を任意に組み合わせるようにしてもよい。

## 【0157】

本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作によって、従来は行われていなかった、最終出力装置である表示装置103への出力経路でのデジタルコンテンツの著作権保護が可能となる。

## 【0158】

そして、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作において、デジタルコンテンツ（表示データ）を単純に暗号化するのではなく、暗号処理の処理対象とするデータを選択し、一部分のみを暗号化するようにしているので、正当な暗号鍵情報105を有していない場合には、元画像の一部分が汚損した状態となる。一部分が汚損されたデジタルコンテンツは、その価値が損なわれるので、デジタルコンテンツの不正コピーを防止することが可能となり、また、デジタルコンテンツの一部分が開示されるので、ユーザの視聴要求を刺激し、デジタルコンテンツの完全な視聴を促すことが可能となる。

## 【0159】

さらに、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作において、デジタルコンテンツの一部分だけを暗号処理の処理対象とし、デジタルコンテンツ全体に対する暗号処理を避けることによって、暗号処理／復号処理の処理量の軽減も可能となっている。なお、汚損度と処理量とはトレードオフの関係にあり、要求に応じて優先度の変更が容易に可能である。

## 【0160】

以上説明したように、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作によって、デジタルコンテンツの出力経路上で著作権を保護しつつ、ユーザの視聴欲求を刺激することが可能となる。

## 【0161】

なお、本実施形態に係る情報処理装置101は、図4に示す構成ではなく、図

1 3 に示す構成にし、図 4 に示した暗号処理部 4 0 1 を、ソフトウェアで実現するようにしてもよい。

【0 1 6 2】

図 1 3 は、本実施形態に係る情報処理装置 1 0 1 の他の概略構成図である。

【0 1 6 3】

図 1 3 でも、図 4 と同様に、P C などの情報処理装置 1 0 1 のうち、表示に関する部分であって、かつ、出力経路暗号化動作に関する部分のみを示している。

【0 1 6 4】

図中、図 4 と同じ構成要素には同じ符号を付与してある。7 0 1 は不揮発性記憶装置である。

【0 1 6 5】

図 1 3 に示す構成の情報処理装置 1 0 1 においては、図 4 に示した暗号処理部 4 0 1 の動作を、C P U 3 0 1 がシステムメモリ 3 0 2 上にプログラムをロードして実行することで実現するものである。すなわち、図 1 3 に示す構成の情報処理装置 1 0 1 は、表示制御装置 3 0 3 ではなく、C P U 3 0 1 が表示データを暗号化するようにしている。

【0 1 6 6】

図 1 4 は、図 1 3 に示す構成の情報処理装置 1 0 1 の概略動作を示す説明図である。

【0 1 6 7】

図 1 4 に示すように、表示メモリ 3 0 4 に蓄積された平文表示データ 8 0 8 は、C P U 3 0 1 の指示に従って、表示制御装置 3 0 3 およびバス 3 0 7 を介してシステムメモリ 3 0 2 に入力される。

【0 1 6 8】

C P U 3 0 1 は、入力した平文表示データ 8 0 8 に対して、暗号鍵情報 1 0 5 を用いて暗号処理 1 0 9 を施す。C P U 3 0 1 によって暗号化された暗号化表示データ 9 0 2 は、バス 3 0 7 および表示制御装置 3 0 3 を介して表示メモリ 3 0 4 に入力される。表示メモリ 3 0 4 に蓄積された暗号化表示データ 9 0 2 は、表示制御装置 3 0 3 によって読み出され、表示装置 1 0 3 に出力される。

## 【0169】

すなわち、図13に示す構成の情報処理装置101においては、CPU301が、表示メモリ304上に平文表示データ808を生成し、さらに、平文表示データ808から表示メモリ304上に暗号化表示データ902を生成する。表示制御装置303は、暗号化表示データ902の読み出し動作を行い、表示動作を行う。

## 【0170】

ここで、暗号鍵情報105は、図4を用いた説明では、表示制御装置303の内部に保持されているものとしたが、図13に示す構成の情報処理装置101においては、暗号鍵情報105は、不揮発性記憶装置701に保持されているものとする。

## 【0171】

また、本実施形態に係る情報処理装置101は、図4および図13のいずれにおいても、情報処理装置102本体と表示装置103とを備えた構成としているが、配布経路暗号化動作で説明したのと同様に、情報処理装置本体102と表示装置103が一体化した構成であってもよい。すなわち、本実施形態に係る情報処理装置101を、いわゆるPDAなどと呼ばれる携帯情報端末としてもよい。

## 【0172】

上述したように、一般に、携帯情報端末は、比較的性能の低いCPUや小容量のメモリなどを用いて構成されることが多いので、比較的重い処理である暗号処理は携帯情報端末にとって大きな負担になるという問題がある。

## 【0173】

そこで、このような問題がある携帯情報端末を、本実施形態に係るデジタルコンテンツ配布システムで用いるようにすれば、全体ではなく一部分が暗号化されたデジタルコンテンツを扱うことにより、本発明が目的とする、著作権保護とユーザの視聴覚欲求刺激の両立を実現することができる上、暗号処理量の低減による負荷低下効果を得ることができる。特に、携帯情報端末が暗号処理をソフトウェアで実現する場合には、暗号処理用に高性能なCPUや大容量メモリを搭載する必要がなくなり、低コスト化、低消費電力化といった効果が得られる。また、

携帯情報端末が暗号処理専用のハードウェアを備えるようにする場合には、暗号処理専用のハードウェアに必要な処理速度が低下することから、低動作速度による低消費電力化、ハードウェア論理の小規模化による低コスト化といった効果が得られる。

## 【0174】

ところで、上述の説明では、デジタル表示装置への出力を例にしたが、必ずしも表示のみを対象としている訳ではない。

## 【0175】

例えば、デジタル入力を持った音声出力装置においても、PCM (Pulse Code Modulation) 符号化された音声データに対して、同様に、数サンプルおきに暗号化を施すことで、出力装置経路暗号化動作を実現することが可能である。

## 【0176】

以上説明したように、本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツのフォーマットに依存する形で、デジタルコンテンツの一部に対して暗号処理を施すようにすることで、正当な暗号鍵情報を有さない場合に、一部が汚損されたデジタルコンテンツとなるようにしている。そこで、デジタルコンテンツの著作権を保護しつつ、ユーザの視聴覚欲求を刺激することが可能となる。

## 【0177】

従って、本実施形態に係るデジタルコンテンツ配布システムによれば、付加価値の高いデジタルコンテンツを、安全に半導体記憶媒体やデジタルネットワーク上で流通させることが可能となり、デジタルコンテンツ配布サービスなどへの応用が可能となる。

## 【0178】

なお、デジタルコンテンツの保護においては、配布経路暗号化動作および出力経路暗号化動作のうちのいずれか一方を用いたシステムとしてもよいし、また、両者を組み合わせ、2つの独立した暗号方式によって、デジタルコンテンツの保護を行うシステムとしてもよい。

## 【0179】



【発明の効果】

以上説明したように、本発明によれば、デジタルコンテンツの著作権を保護しつつ、ユーザの視聴覚欲求を刺激することの可能な、デジタルコンテンツの最終出力が可能となる。

【図面の簡単な説明】

【図 1】 本実施形態に係るデジタルコンテンツ配布システムの概略構成図。

【図 2】 本実施形態に係るデジタルコンテンツ配布システムの概略動作フローチャート。

【図 3】 本実施形態に係る情報処理装置の概略構成図。

【図 4】 本実施形態に係る情報処理装置の概略構成図。

【図 5】 デジタルコンテンツ配布装置から配布されるデジタルコンテンツの暗号化方法の一例を示す説明図。

【図 6】 図 5 に示す暗号化方法で暗号化されたデジタルコンテンツを表示装置で表示した場合の表示イメージを示す説明図。

【図 7】 本実施形態に係る情報処理装置の概略構成図。

【図 8】 本実施形態に係る表示制御装置の概略構成図。

【図 9】 本実施形態に係る表示装置の概略構成図。

【図 1 0】 本実施形態に係る表示装置の概略構成図。

【図 1 1】 表示制御装置から出力される表示データの暗号化方法の一例を示す説明図。

【図 1 2】 表示制御装置から出力される表示データの暗号化方法の一例を示す説明図。

【図 1 3】 本実施形態に係る情報処理装置の概略構成図。

【図 1 4】 図 1 3 に示した情報処理装置の概略動作を示す説明図。

【符号の説明】

- 1 0 0 : デジタルコンテンツ配布装置
- 1 0 1 : 情報処理装置
- 1 0 2 : 情報処理装置本体
- 1 0 3 : 表示装置

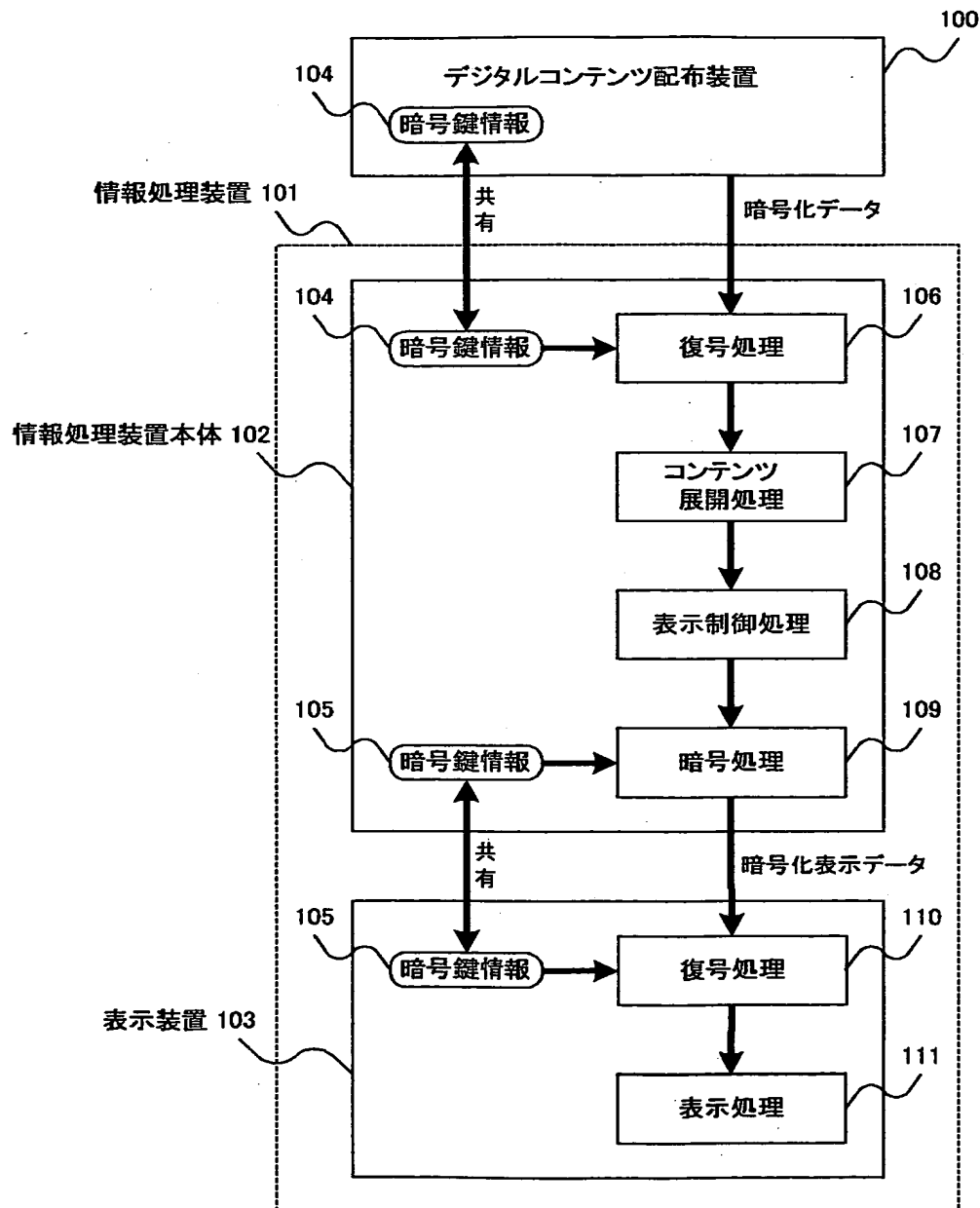
1 0 4 : 暗号鍵情報  
1 0 5 : 暗号鍵情報  
1 0 6 : 復号処理  
1 0 7 : コンテンツ展開処理  
1 0 8 : 表示制御処理  
1 0 9 : 暗号処理  
1 1 0 : 復号処理  
1 1 1 : 表示処理  
3 0 1 : 中央演算装置 (CPU : Central Processing Unit)  
3 0 2 : システムメモリ  
3 0 3 : 表示制御装置  
3 0 4 : 表示メモリ  
3 0 5 : 入力制御装置  
3 0 6 : 通信制御装置  
3 0 7 : バス  
3 0 8 : 復号処理部  
3 0 9 : コンテンツ展開処理部  
4 0 1 : 暗号処理部  
4 0 2 : 復号処理部  
4 0 3 : データドライバ  
7 0 1 : 不揮発性記憶装置  
8 0 1 : メモリ制御部  
8 0 2 : タイミング生成部  
8 0 3 : タイミング信号  
8 0 4 : メモリ制御信号  
8 0 5 : メモリアドレス信号  
8 0 6 : LCD (Liquid Crystal Display) 制御部  
8 0 7 : LCD 制御信号  
8 0 8 : 平文表示データ

809 : タイミング制御部  
810 : LCD表示データ  
811 : シリアル／パラレル変換回路 (S／P回路)  
812 : S／P済LCD表示データ  
813 : 暗号化S／P済LCD表示データ  
814 : パラレル／シリアル変換回路 (P／S回路)  
815 : 暗号化LCD表示データ  
816 : 遅延回路  
817 : 遅延済LCD制御信号  
901 : CL2信号  
902 : 暗号化表示データ  
903 : CL1信号  
904 : LCD駆動用電源  
905 : 液晶駆動出力信号  
906 : ラッチアドレスセクタ  
907 : ラッチ回路－1  
908 : ラッチ回路－2  
909 : レベルシフタ  
910 : 液晶駆動回路  
911 : ラッチ回路－3  
912 : 平文表示データ  
1001 : S／P回路  
1002 : P／S回路  
1003 : S／P済表示データ  
1004 : 平文表示データ

【書類名】 図面

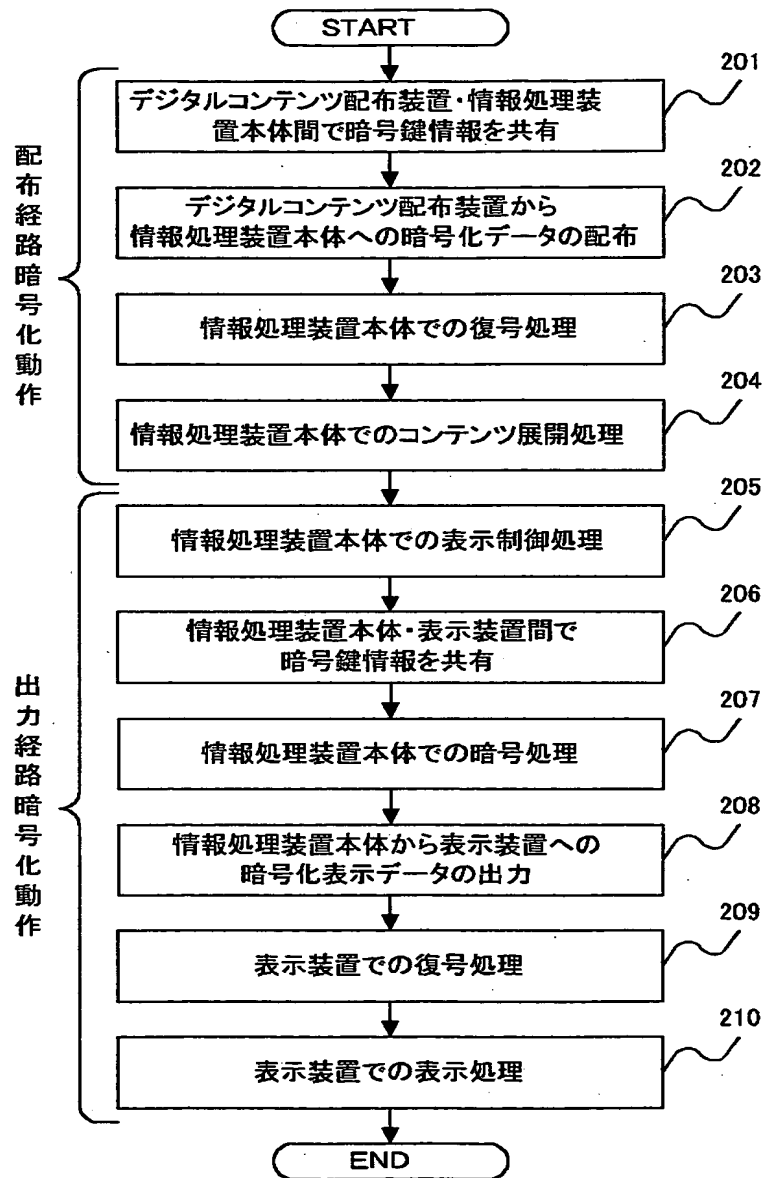
【図 1】

図 1

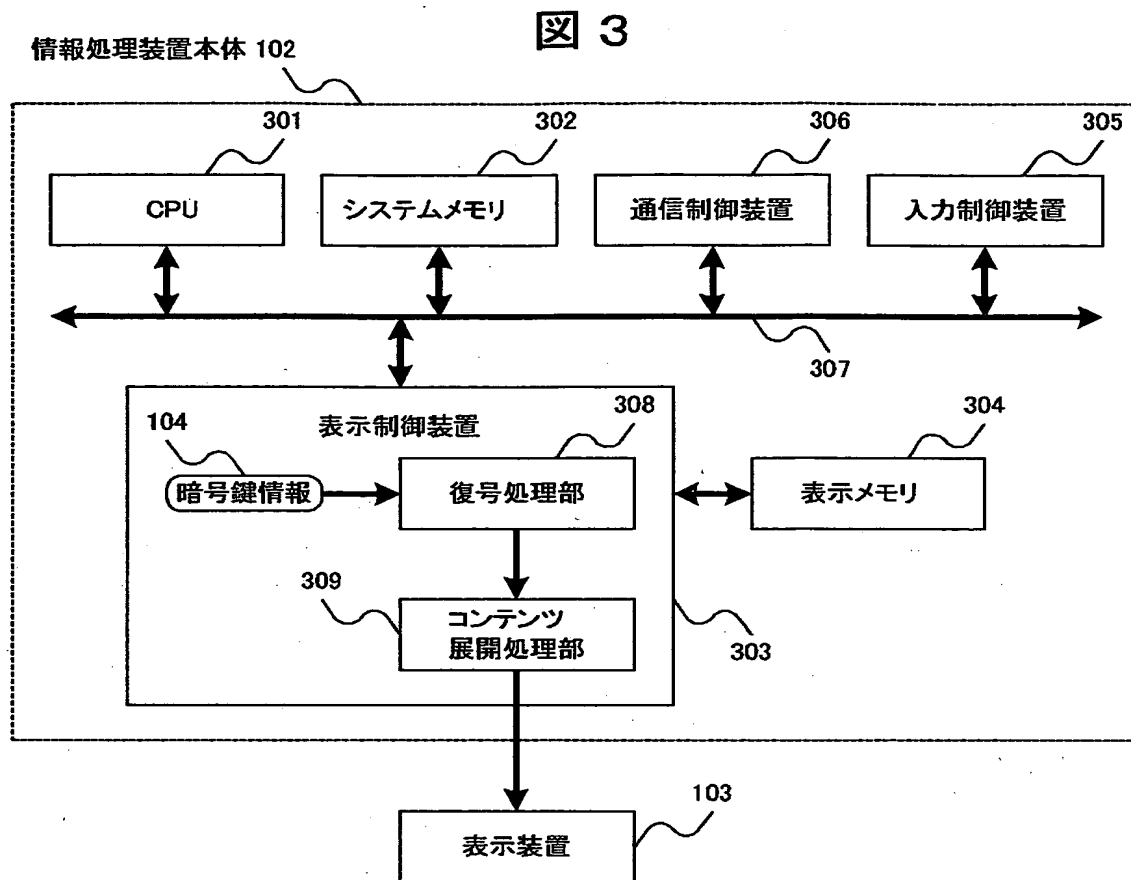


【図 2】

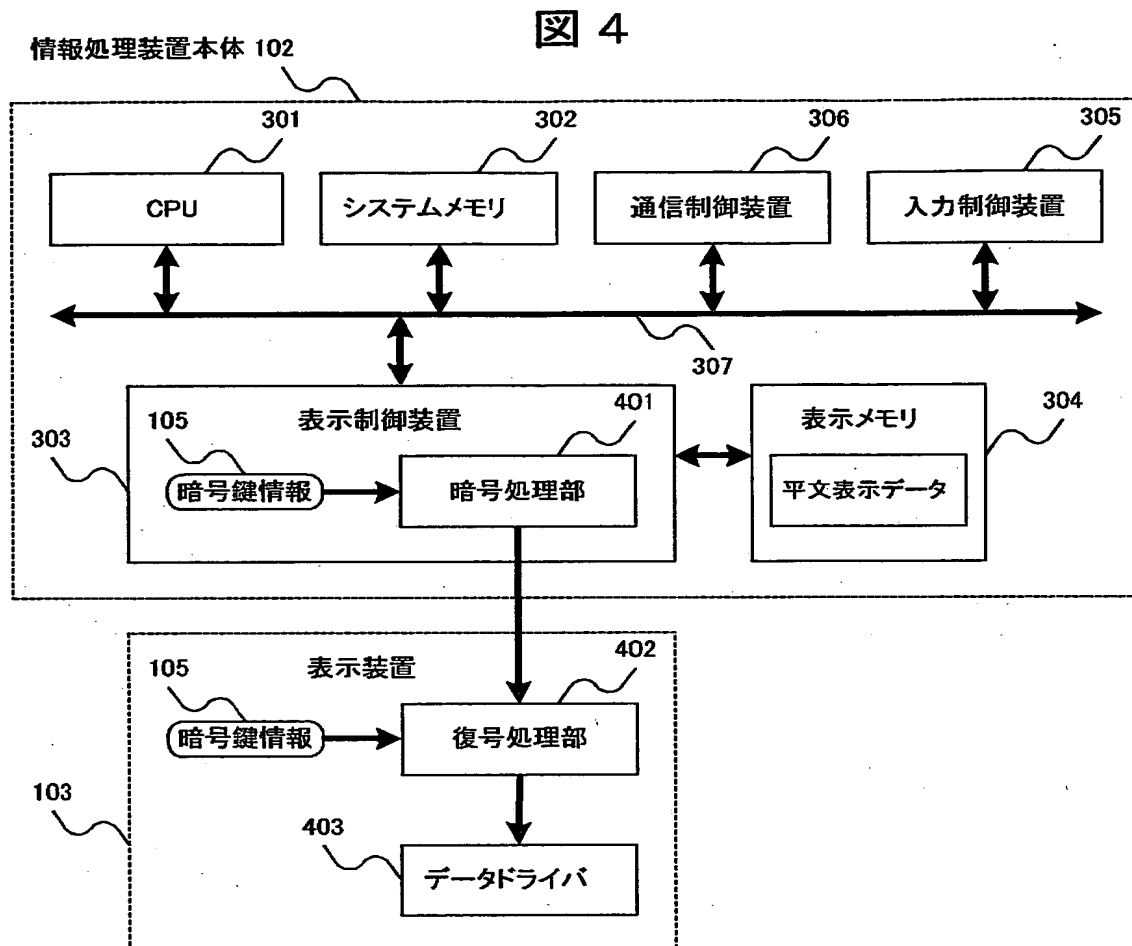
図 2



【図 3】



【図 4】



【図 5】

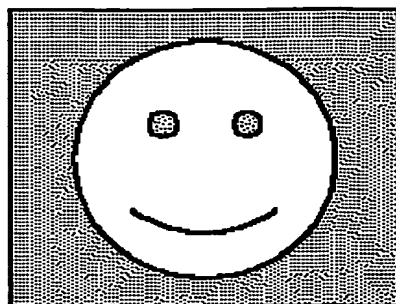
図 5

暗号化対象	暗号鍵情報なしに得られる ピクチャデータ			符号割り当て量 @ピクチャデー タ	暗号処理量 @ピクチャデー タ
	I	P	B		
Iピクチャデー タ	×	×	×	大	大
Pピクチャデー タ	○	×	×	中	中
Bピクチャデー タ	○	○	×	小	小

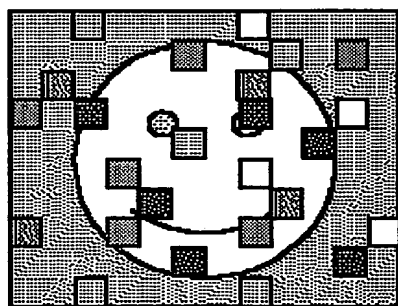
【図 6】

図 6

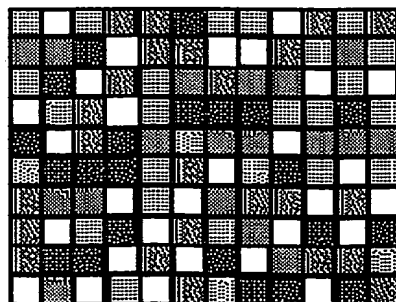
(a)



(b)

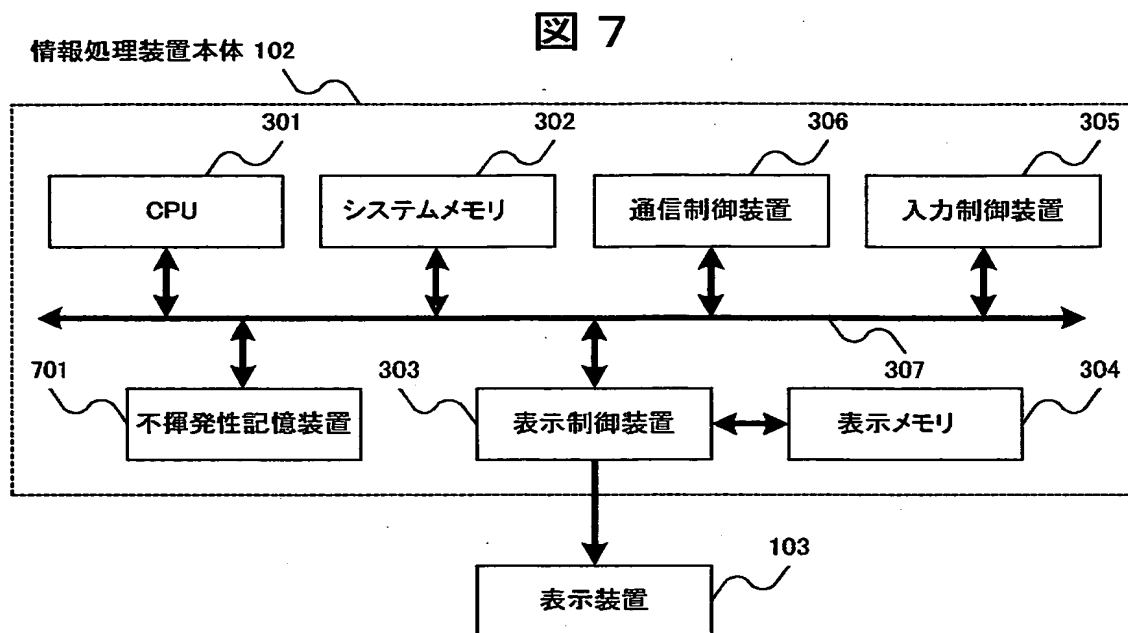


(c)

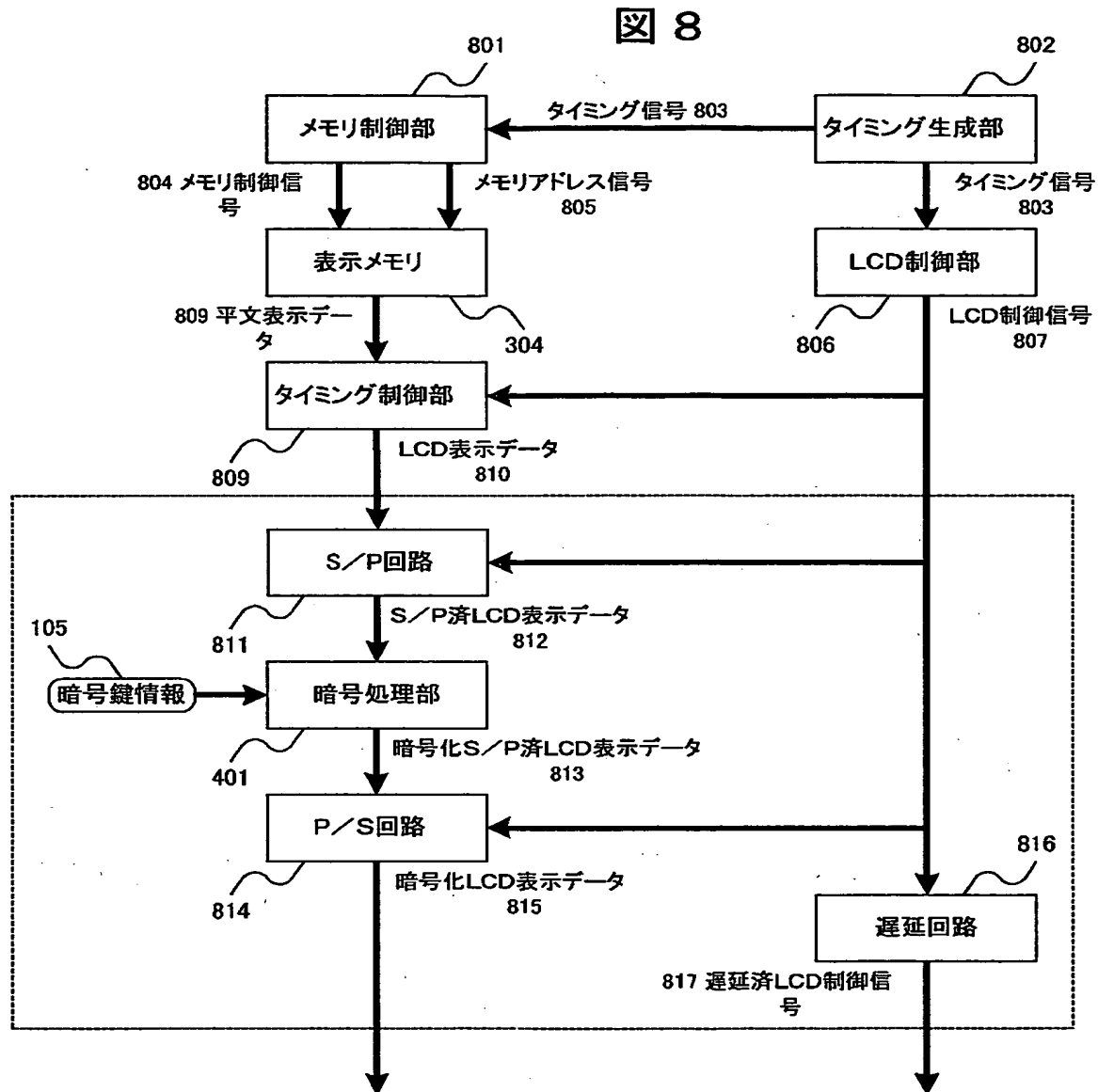




【図 7】

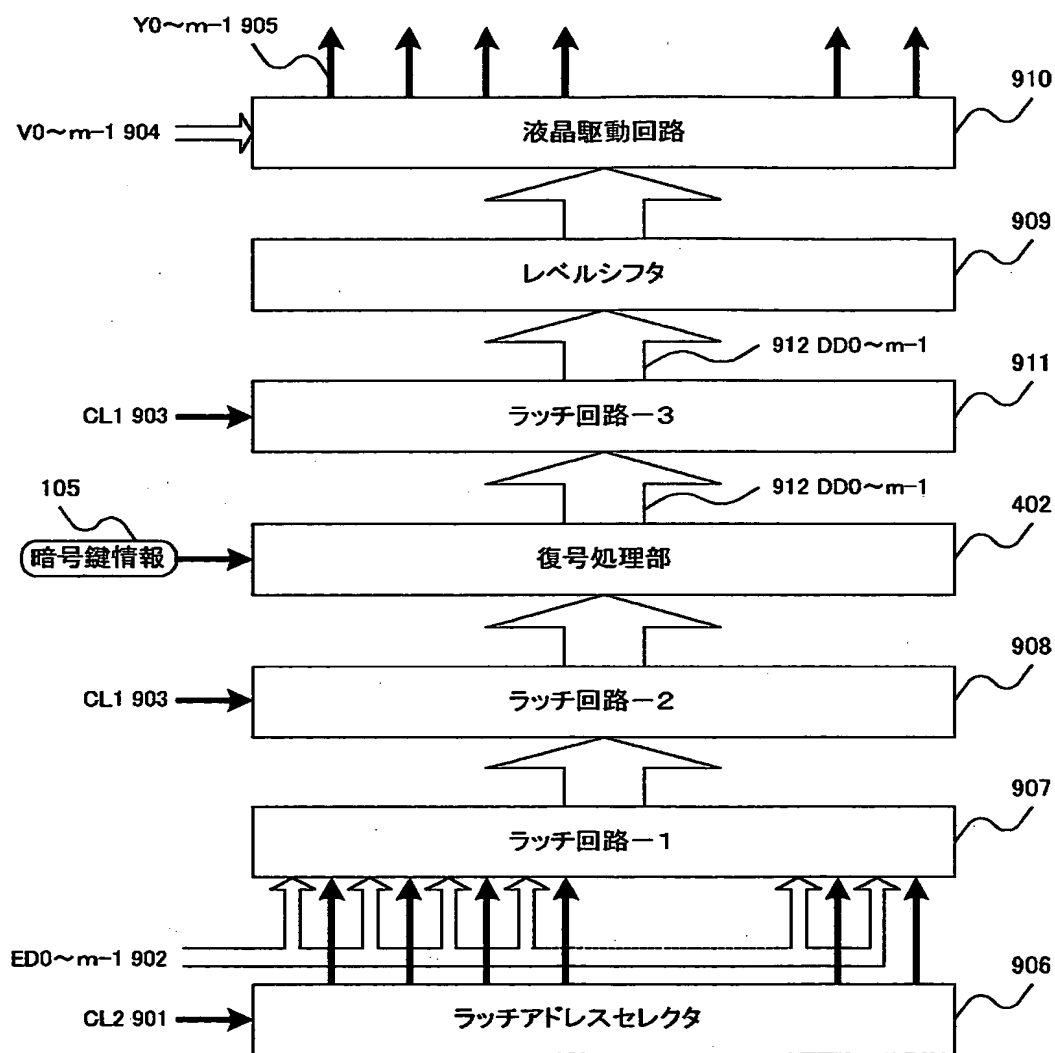


【図 8】



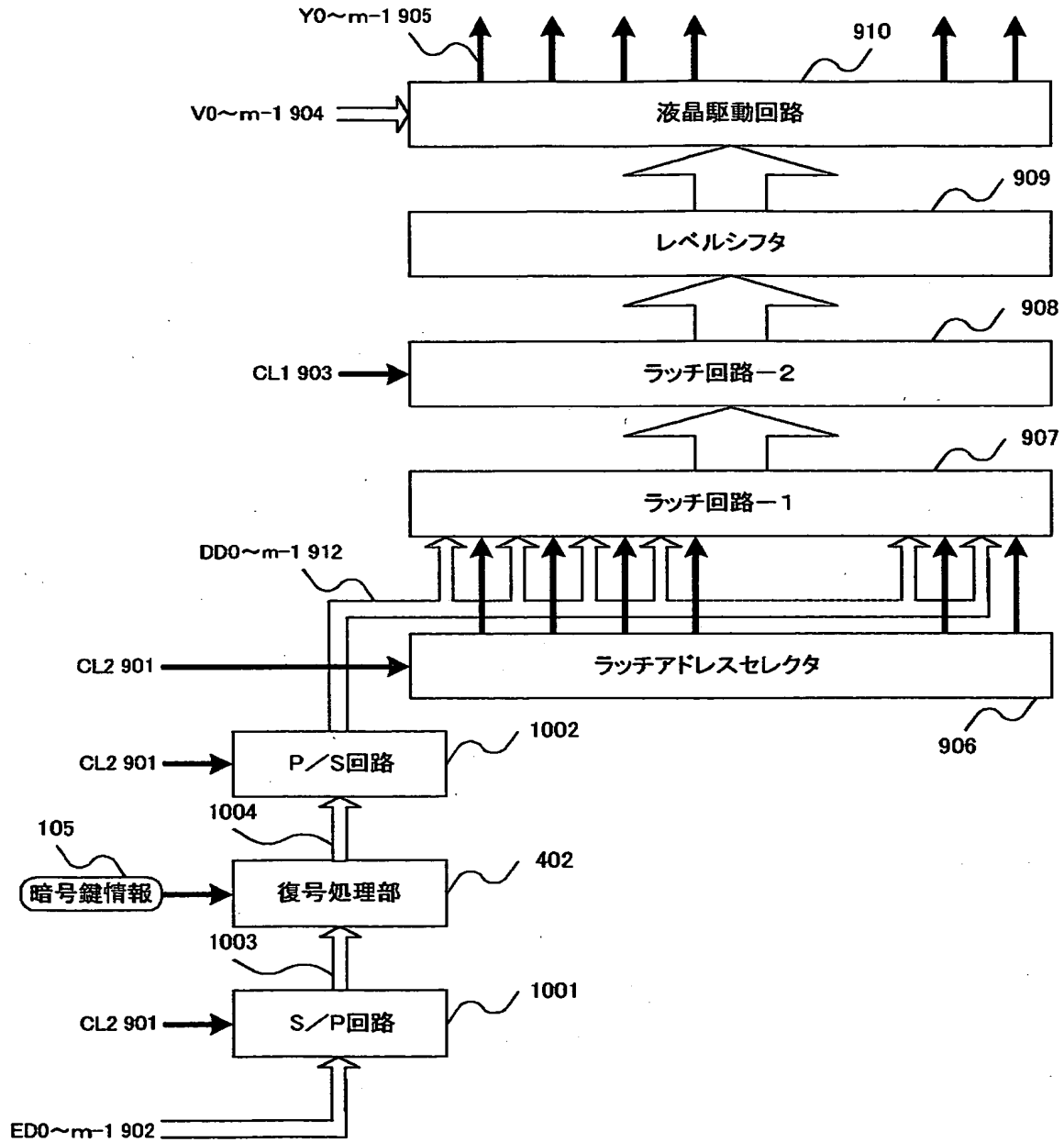
【図 9】

図 9



【図10】

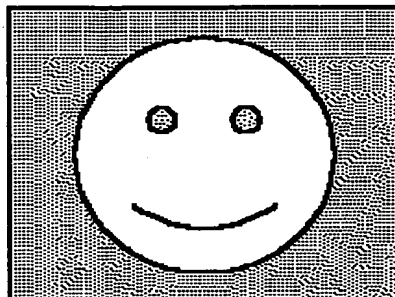
図 10



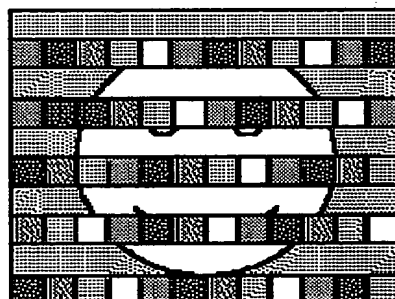
【図 1 1】

図 1 1

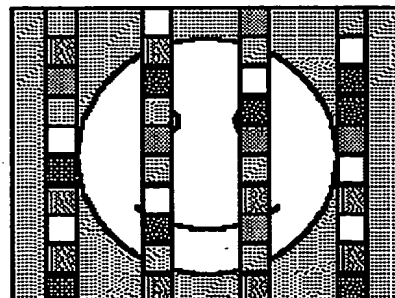
(a)



(b)



(c)



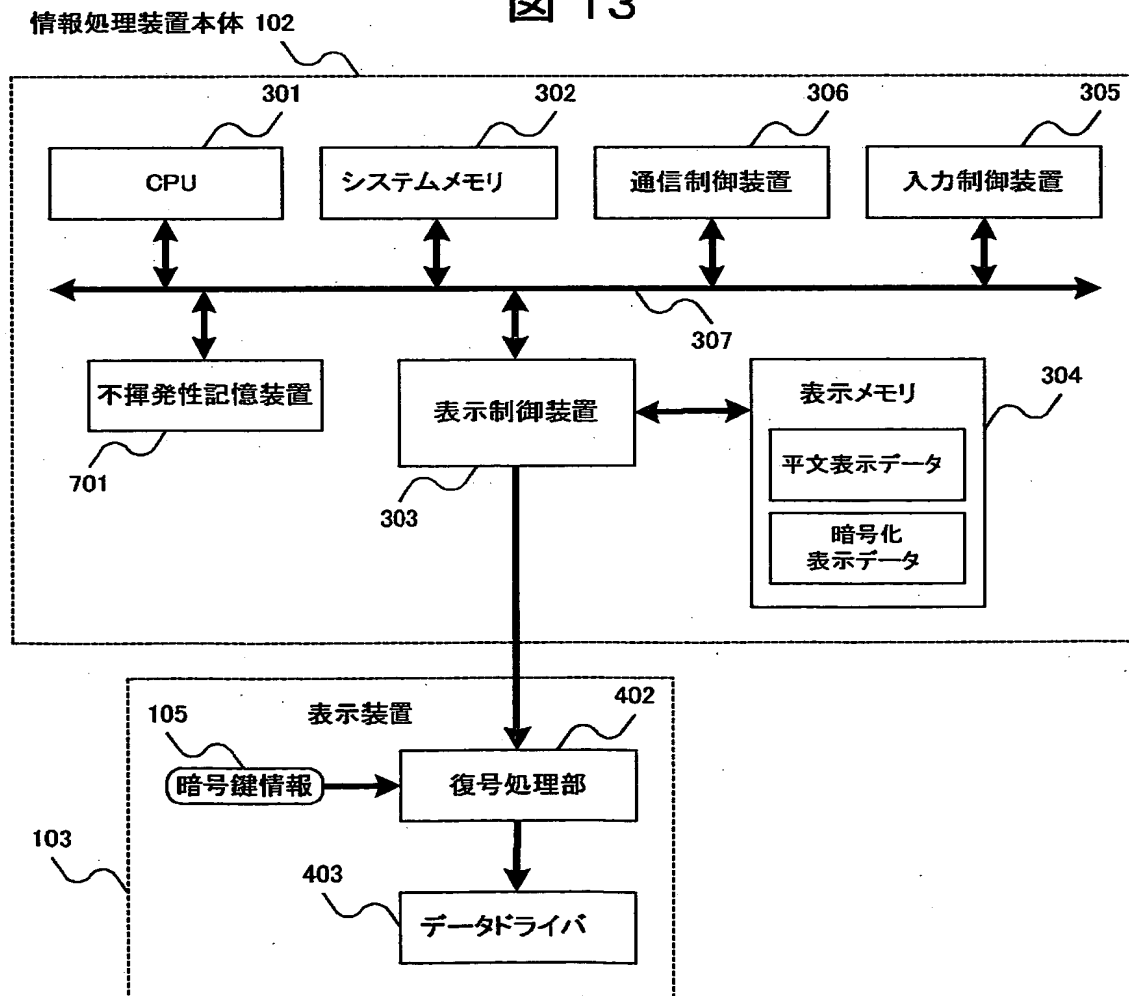
【図 1 2】

図 12

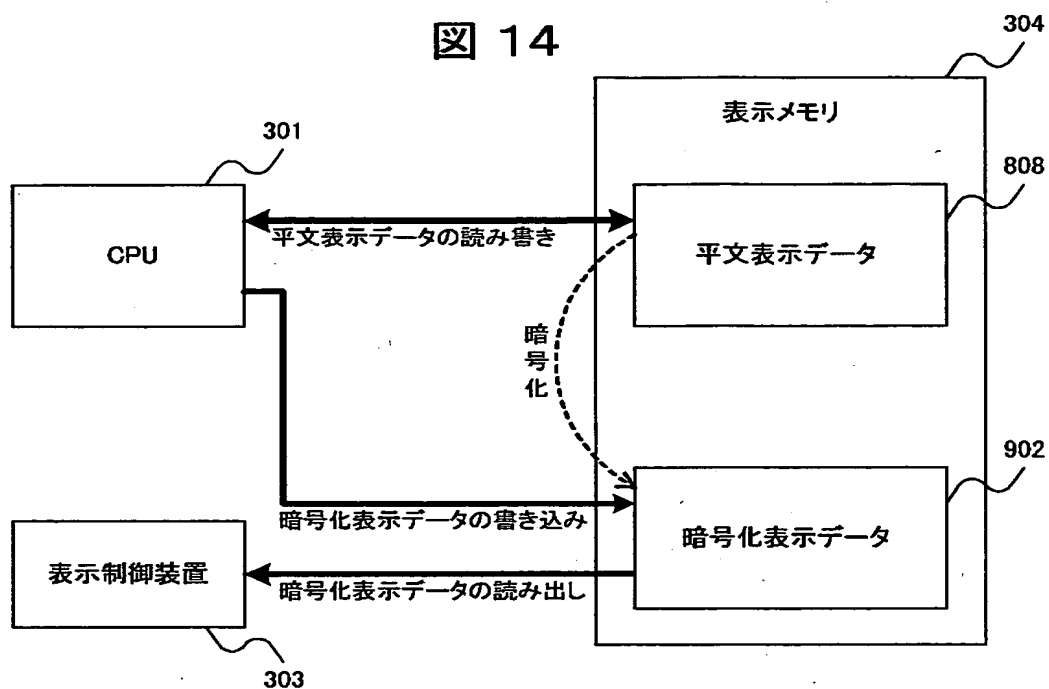
	MBS		LBS						
平文	0	1	0	1	0	1	0	1	=55h
上位ビット暗号化	1	1	1	0	0	1	0	1	=e5h
下位ビット暗号化	0	1	0	1	0	0	1	0	=52h

【図 1 3】

図 13



【図 1 4】



【書類名】要約書

【課題】デジタルコンテンツの権利を保護しつつ、ユーザの視聴覚欲求を刺激する形でのデジタルコンテンツの最終出力を可能とする。

【解決手段】情報処理装置本体 1 0 2 が、表示装置 1 0 3 と共有する暗号鍵情報 1 0 5 を用いて暗号化したデジタルコンテンツ（表示データ）を、表示装置 1 0 3 に転送し、表示装置 1 0 3 が、情報処理装置本体 1 0 2 から転送される表示データに対して、暗号鍵情報 1 0 5 を用いて復号処理を施すようにしている。ここで、情報処理装置本体 1 0 2 から表示装置 1 0 3 に転送される表示データは、例えば、数ライン分おきに、数ライン分の表示データずつが暗号化されるなど、一部分のみが暗号化されたものである。

【選択図】図 1



出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台4丁目6番地
氏 名	株式会社日立製作所